REMARKS

35 U.S.C § 102

The examiner rejected Claims 1-3, 5, 7-16, 18-22, and 28-32 under 35 U.S.C. 102 (e) as being anticipated by Ontiveros et al. (U.S. Pub 20020107953).

The examiner stated:

> **As per claim 1, Ontiveros discloses a system, comprising:**
> **a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network (paragraph [0024])**
> **an aggregator device that receives the connection information from the plurality of collector devices (paragraph [0037]), and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node (paragraph [0040]), with the aggregator device further comprising:**
> **a process executed on the aggregator device to detect anomalies in connection patterns (paragraphs [0008] and [0024])**
> **a process executed on the aggregator device to aggregate detected anomalies into the network events (paragraph [0026], Anomaly Detection System) with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies (paragraphs [0003] and [0024]).**

Claim 1 is distinct over Ontiveros. Claim 1 includes the features of ... an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to and from the node, ... the aggregator device to detect anomalies in connection patterns and ... to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies.

The examiner in response to Applicant's prior Reply stated:

> **As per claims 1, and 14, in response to applicant's arguments that Ontiveros fails to disclose a connection table that maps each node of a network to a record that stores information about packet traffic to or from the node, the Examiner respectfully disagrees and would like to point out to paragraph [0037] wherein Ontiveros discloses "...the preferred packet daemon creates memory references to each packet source Media Access Control (MAC) address in a hash table, wherein keys (which are the part or group of the data by which it is sorted, indexed and cataloged), are mapped to array positions."**

Applicant further argues that Ontiveros fails to disclose a process executed on the aggregator device to detect anomalies in connection patterns. The Examiner respectfully disagrees and would like to point out to paragraphs [0043] through [0050], wherein Ontiveros discloses sorting data by Source Address, Destination Address, and Source Destination Address...Using these primary data types, the present invention can sort data type attacks and protocol types to identify new patterns, as well as catalog usage patterns and usage profiles. Using the keys, a hash table can be created to monitor for and determine data attack types depending upon the particular security needs of the network. Monitoring source and destination address (i.e. host to host connections) and identifying certain patterns reads on the claimed limitation.

Applicant further argues that Ontiveros fails to disclose a process executed on the aggregator device to aggregate detected anomalies into the network events. The Examiner respectfully disagrees and would like to point out to paragraph [0024] wherein Ontiveros discloses monitoring and detecting patterns that are in contrast to normal traffic patterns. Thus detecting events associated with attacks.

Applicant's claim 1 is directed to using connection information in a connection table in detection of anomalies that can include denial of service attack and scanning attack anomalies. Ontiveros does not produce the claimed connection table.

The examiner relies principally on [0037] from Ontiveros to disclose the claimed connection table. Specifically, the examiner explains in response to Applicant's prior argument that: "**the Examiner respectfully disagrees and would like to point out to paragraph [0037] wherein Ontiveros discloses "...the preferred packet daemon creates memory references to each packet source Media Access Control (MAC) address in a hash table, wherein keys (which are the part or group of the data by which it is sorted, indexed and cataloged), are mapped to array positions**"

Applicant however points out that memory references are not a connection table. Ontiveros Fig. 2 is reproduced below:

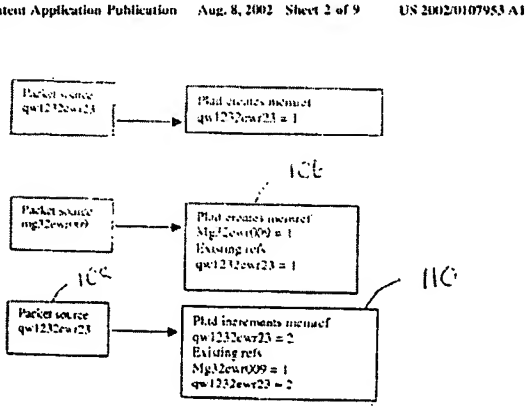

FIG. 2

As explained by Ontiveros the memory references are storage areas for packets in memory with a particular, e.g., source address. Ontiveros describes these memory references as:

> **For example, as shown at 100 in FIG. 2, the packet daemon identifies the packet source address qw1232ewr23 and at 102 creates a memory reference (memref) for that source address. At 104 the packet daemon identifies the source address of the next data packet traversing the port being monitored by the packet daemon, in FIG. 2, the source address being mg32ewr009. At 106 another memref is created for this source address. Therefore, at 104 each of the memrefs are equal to 1, representing that one data packet from each of the sources identified has traversed the data port of interest.**

Nothing in Fig. 2 paragraph [0037] or elsewhere shows that Ontiveros described the claimed connection table. That is, the structures of Fig. 2 are not a record that stores information about packet traffic to and from the node.

This is contrasted with Applicant's FIG. 4 a pictorial view of a connection table

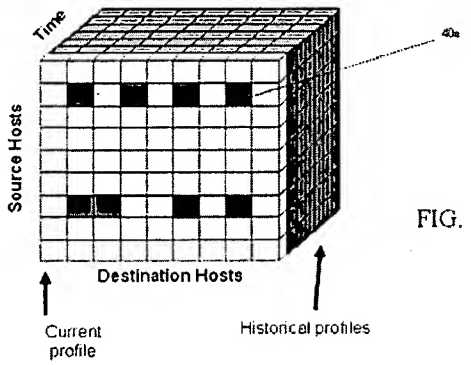

FIG. 4

and FIG. 5 a representation of a record in the connection table. As can be seen by the diagrammatical view of FIG. 4 the indices of the table are as source and destination hosts over time periods.

In contrast Ontiveros teaches at [0038] "**A "hit-count" table is preferably created in memory to count the number of times a particular pair of source and destination IP addresses is detected.**" Applicant contends that the teachings relied on by the examiner, namely [0037] are directed to this so called hit-count table which as Ontiveros describes keeps a count of the number of times a particular pair of source-destination addresses are detected.

However, nowhere does Ontiveros describe any structure similar to the record below:

Time Slice	Fri	Thu	Wed	.	Sun	Sat	Fri
Services provided by A (Web Server) to B (Desktop)							
WWW (TCP:80)							
Bytes / sec	2k	3k	1k	...	2k	4k	3k
Packets / sec	5	6	2		5	9	5
Conn's. / hr	.3	.5	.3		.2	.3	.3
SSH (TCP:22)							
Bytes / sec	1k	3k	4k	...	1k	2k	3k
Packets / sec	2	6	9		2	5	6
Conn's. / hr	.3	.5	.3		.3	.3	.5
				...			
Services provided by B (Desktop) to A (Web Server)							
SSH (TCP:22)							
Bytes / sec	21k	0	0	...	0	0	0
Packets / sec	10	0	0		0	0	0
Conn's. / hr	1	0	0		0	0	0

FIG. 5

Therefore, Ontiveros cannot be construed to describe or suggest "a connection table that maps each node on the network to a record that stores information about packet traffic to and from the node."

There are other distinguishing features of claim 1 over Ontiveros that were addressed by Applicant in the previous reply, e.g., detect anomalies in connection patterns, and which Applicant contends are still valid.

Claims 12-13

The examiner also reply to Applicant's arguments that: "**As per claims 12 and 13, applicant argues that Ontiveros fails to disclose the connection sub-tables include a time-slice connection table. The Examiner respectfully disagrees and would like to point out to paragraph [0040]-[0042] wherein Ontiveros discloses user defined time intervals.**"

Applicant notes that Ontiveros mentions a user defined sample time. However nothing in those paragraphs or elsewhere describes or suggests that the connection table includes a plurality of connection sub-tables to track data at different time scales, or as in claim 13 that the connection sub-tables include a time-slice connection table that operates on a small unit of time and at least one other sub-table that operates on a larger unit of time than the time slice sub-table

with each sub-table holding the sum of records received from all collectors during respective units of time.

A sampling period by itself does not suggest that the hit count table of Ontiveros tracks data at different time scales or that the hit count table has a sub-table that operates over a small unit of time and one sub-table that operates on a larger unit of time each sub-table holding the sum of records received from all collectors during the respective units of time.

Comments on Statement of Reasons for Allowance

The examiner indicated allowable subject matter with respect to claims 23, 24 and claims 33-36 and thus withdrew the previous 102(b) rejection of claims 23 and 24.

The examiner stated:

> **In response to applicant's arguments regarding claims 23-24, and 33-34 after a complete search of all the relevant prior art the examiner has determined the claims are in condition for allowance. The following limitations when viewed in combination with the remainder of the claim as a whole place this application in condition for allowance.**
>
> **As per claims 23 and 33, the Examiner finds the novel and non obvious feature of claim, when read as whole to be detecting a new host connecting to a network comprises receiving statistics collected from a host in the network and indicating to a console that the host is a new host if, during a period of time T, the host transmits at least N packets and receives at least N packets, and if the host had never transmitted and received more than N packets in any previous period of time with a duration of T.**
>
> **As per claims 24 and 34, the Examiner finds the novel and non obvious feature of claim, when read as whole to be detecting a failed host in a network comprises determining if both a mean historical rate of server response packets from a host is greater than M, and a ratio of a standard deviation of historical rate of server response packets from the host to a mean profiled rate of server response packets from the host is less than R over a period of time; and indicating the host as a potential failed host if both conditions are present.**

Applicant does not necessarily disagree with these comments but contends that other reasons for allowance may also exist. For example, Applicant points out that the examiner ins the summary of the rejection indicated that claims 23-27 were also allowable, but did not specifically reflect that claims 25-27 were allowed in the examiner's comments.

Applicant contends that the case is in condition for allowance and such action is requested.

This Reply is accompanied by a Notice of Appeal.

The fee of **$245** for the Petition for Extension of Time is being paid electronically on the electronic filing system by way of deposit account authorization. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: December 18, 2008

/Denis G. Maloney/
Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

22085656.doc